IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	
	)	
RASHAWN ERIC MCEACHERN	)	1:21-CR-418

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED IN VIOLATION OF DEFENDANT'S FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SEARCHES AND SEIZURES

Rashawn Eric McEachern, by and through his attorney, helen Parsonage, respectfully submits this Motion to Suppress evidence obtained as a result of an unreasonablesearch. As grounds, it is stated:

1. Mr. McEachern is charged with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2)(A), (b)(1), and one count of possession of child pornography involving a minor who had not attained 12 years of age in violation of18 U.S.C. § 2252(a)(5)B), (b)(2).

2. The charges stem from a search of Mr. McEachern's home that he contends wasconducted in violation of his Fourth Amendment right against unreasonable searches.

3. Mr. McEachern owns and operates a General Public License version of lawful peer-to-peer software called ‘Freenet’.

4. Freenet is peer-to-peer data sharing software built for anonymity. To retrieve a file from the software, a user must request pieces of that file from other users. The pieces are collected and assembled to create the file intended. Requests are forwarded from peer-to-peer up to eighteen times. As such, it is difficult to know whether or not the requesting peer is the original requestorof the file, or simply one forwarding a request.

5. The North Carolina State Bureau of Investigation (“NCSBI”) owns and operates a modified version of Freenet which stores information, including IP addresses, of other Freenet users it connects to.

6. The NCSBI’s computer running its version of Freenet received a number of requests fromthe same IP address requesting segments of files of child pornography on September 20, 2021 and October 17, 2021.

7. The number of file segments indicated to law enforcement to target the IP address sending the requests. Law enforcement

conducted an analysis upon each request using an algorithm. As a result, NCSBI Agents believed that the IP address was most likely the original requestor for each file.

8. Mr. McEachern asserts that the NCSBI's method of determining which requests warrants indicate possession of child pornography is arbitrary and unreliable.

9. The methodology used by the NCSBI did not, with sufficient accuracy, determine whether Mr. McEachern was necessarily the original requestor of the files such that law enforcement officers had probable cause to search Mr. McEachern's home.

10. Law enforcement determined that the IP address requesting the files mentioned above was controlled by Charter Communications. On September 22, 2021, an administrative subpoena was sent to Charter for subscriber information relating to the IP address. Charter provided information that the IP address belonged to Rashawn McEachern.

11. On October 21, 2021, law enforcement executed a search warrant on Mr. McEachern's home and seized Mr. McEachern's desktop, and external hard drives.

12. The Fourth Amendment guarantees rights to be free from unreasonable searches and seizures.

13. In order to constitutionally search Mr. McEachern's home, law enforcement were required to obtain and articulate a basis of probable cause. There was not a sufficient basis forprobable cause to search Mr. McEachern's home.

14. "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Maryland v. Pringle*, 540 U.S. 366, 370-71 (2003). "To determine whether an officer had probable cause to arrest an individual, we examine the events leading up to the arrest, and then decide "whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to" probable cause." *Id*. The standard "deals with probabilities and depends on the totality of the circumstances." *Id.* at 371.

15. Evidence obtained as a result of an unreasonable search in violation of the Fourth Amendment may be subject to the exclusionary rule. The exclusionary rule is intended to deter police misconduct and protect the privacy rights of individuals; "If exclusion of evidence

obtained pursuant to a subsequently invalidated warrant is to have any deterrent effect… it mustalter the behavior of individual law enforcement officers or the policies of their departments." *United States v. Leon*, 468 U.S.897, 918 (1984).

16. The Court must balance "the benefits of the rule's deterrent effects against the costs of exclusion, which include 'letting guilty and possibly dangerous defendants go free.' " *United States v. Tracey,* 597 F.3d 140, 151 (3d Cir.2010) (quoting *Herring,* 555 U.S. at 141, 129 S.Ct. 695).

17. Mr. McEachern asserts that law enforcement did not have a basis of probable cause tosearch his home or his electronic devices on October 21, 2021.

WHEREFORE, for the reasons set forth in the accompanying Memorandum of Law, as well as any which may become apparent at a hearing or the Court deems just, Defendant Rashawn McEachern, by his counsel undersigned, respectfully requests that the Court grant his Motion andpreclude the government from introducing all evidence seized on October 21, 2021.

Respectfully submitted, this the 22nd day of March 2022

/s/Helen L. Parsonage
Helen L. Parsonage (35492)
Elliot Morgan Parsonage, PLLC
426 Old Salem Road
Winston-Salem, NC 27101
(336) 724-2828
hparsonage@emplawfirm.com

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	
	)	
RASHAWN ERIC MCEACHERN	)	1:21-CR-418

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED IN VIOLATION OF DEFENDANT'S FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SEARCHES AND SEIZURES

Mr. McEachern is charged with one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2)(A), (b)(1), and one count of possession of child pornography involving a minor who had not attained 12 years of age in violation of 18 U.S.C. § 2252(a)(5)B), (b)(2). The charges stem from a search of Mr. McEachern's computer that he contends was conducted in violation of his Fourth Amendment right against unreasonable searches. Law enforcement received requests for media files containing child pornography through a peer-to- peer data sharing software. They concluded that the file requests originated from Defendant's computer. That unsupported conclusion, alone, is insufficient to warrant a finding of probable cause; therefore, the subsequent search was conducted in violation of the Fourth Amendment. The defense moves to exclude all evidence obtained as a result of the search from introduction into evidence at trial.

I. BACKGROUND

Mr. McEachern owns and operates a General Public License version of a peer-to-peer software called 'Freenet'. Freenet software is a peer-to-peer data sharing software built for anonymity and censorship free communication, wherein users, or 'peers', upload files that are broken down into chunks and stored on multiple other peer computers. To retrieve a file from the software, a user must request pieces of that file from other users which are collected and assembled to create the file intended. Requests are forwarded from peer to peer up to eighteen times to gather all the necessary pieces. As such, it is difficult to know whether or not a requesting peer is the original requestor of the file, or simply one forwarding a request made by another peer.

The North Carolina State Bureau of Investigation (NCSBI) owns and operates a modified version of Freenet which stores information, including IP addresses, of other Freenet users. The NCSBI's computer running its version of Freenet received a number of requests from the same IP address requesting segments of files of child pornography on September 20, 2021 and October 17, 2021.

Law enforcement conducted an analysis upon these requests, determining whether the IP address requesting the subject files was the original requestor or a forwarding requestor. As a result, NCSBI Agents came to believe that the IP address was most likely the original requestor for each file and used this algorithm as the basis for probable cause.

Law enforcement determined that the IP address requesting the files mentioned above was controlled by Charter Communications. On September 22, 2021, an administrative subpoena was sent to Charter for subscriber information relating to the IP address. Charter provided information that the IP address belonged to Rashawn McEachern.

On October 21, 2021, law enforcement executed a search warrant on Mr. McEachern's home and seized Mr. McEachern's desktop, and external hard drives.

II. DISCUSSION

There is no bright line rule for probable cause; the Supreme Court has "rejected rigid rules, bright-line tests, and mechanistic inquiries in favor of a more flexible, all-things- considered approach." *Florida v. Harris*, 568 U.S. 237, 244 (2013). However, courts' interpretations of what evidence *is* sufficient for probable cause are extensive and instructive. The process and algorithm by which the FBI identified Mr. McEachern's IP address and concluded that he was likely the original requestor does not rise to the level of probable cause justifying a search of his home and electronic devices.

A. Legal Standard

The Fourth Amendment guarantees an individual's right to be free from "unreasonable searches and seizures." U.S. Const. Amend. IV. Absent a finding of probable cause supporting a valid search warrant, the search of Mr. McEachern's home and/or electronic devices was unconstitutional. In this case, Agents did obtain a search warrant after submitting an Affidavit of Probable Cause authored by NCSBI Agent R.V. White. *See* Exhibit A, attached hereto.

"[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Maryland v. Pringle*, 540

U.S. 366 (2003). 370-71. "To determine whether an officer had probable cause to arrest an individual, we examine the events leading up to the arrest, and then decide "whether these historical facts, viewed from the standpoint of an objectively reasonable police officer, amount to" probable cause." *Id*. The standard "deals with probabilities and depends on the totality of the circumstances." *Id.* at 371.

Although reviewing courts give "great deference" to a magistrate's determination of probable cause, "[d]eference to the magistrate . . . is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984). A reviewing court must first inquire "into the knowing or reckless falsity of the affidavit on which that determination was based." *Id*., citing *Franks*, 438 U.S.

"Second, the courts must also insist that the magistrate purport to 'perform his neutral and detached function and not serve merely as a rubber stamp for the police.'" *Id*., quoting *Aguilar v. Texas*, 378 U.S. 108, 111 (1964); see also *Illinois v. Gates*, 462 U.S. 213, 239 (1983). "Third, reviewing courts will not defer to a warrant based on an affidavit that does not 'provide the magistrate with a substantial basis for determining the existence of probable cause.'" *Leon*, 468 U.S. at 915, quoting *Gates*, 462 U.S. at 239; see also *United States v. McArthur*, No. 4:07CR651-DJS, 2008 WL 481993, at *5 (E.D. Mo. Feb. 19, 2008), aff'd, 573 F.3d 608 (8th Cir. 2009).

The methods utilized by the NCSBI did not, with sufficient accuracy, determine whether Mr. McEachern's IP address was actually the original requestor of the files such that agents had probable cause to search his home. This case presents this Court an opportunity to protect individuals from unreasonable searches in a relatively new field.

B. Freenet Background

"Freenet is a platform for censorship-resistant communication and publishing. It is designed to ensure true freedom of communication over the Internet." The Freenet Project, *About*, (2019) *https://freenetproject.org/pages/about.html*. "Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is. Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files." *Id.*

Freenet is a legal tool for the free exchange of information. The creators of Freenet address any question of legality head on. On the Freenet website, the creators have included language that reads

> We don't currently know of any prosecutions for merely using Freenet…ACTA [Anti- Counterfeiting Trade Agreement] might have wide-ranging effects, including on Freenet, should it pass… There have also been attempts to force peer to peer systems to provide wiretapping capabilities in the USA, and there are worrying developments in the UK that might result in it being blocked, but not being made illegal per se. As far as we know none of these things… have passed. Many of these are arguable either way (depending on how broadly the legislation is applied) and will have to be decided in caselaw.

The Freenet Project, *Help*, (2019) *https://freenetproject.org/pages/help.html*. The creators make it clear that they did not intend for any illegality to be connected to their software. They state that

> We have done everything we can to make it extremely difficult for any sane legal system to justify punishing someone for running a Freenet node, and there is little precedent for such action in today's developed countries. Many legal systems recognize the importance of freedom of speech, which is Freenet's core goal.

Id. The process by which Freenet operates is described below:

> Users contribute to the network by giving bandwidth and a

> portion of their hard drive (called the "data store") for storing files. Files are automatically kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can't be held accountable for it.

The Freenet Project, *About*, (2019) *https://freenetproject.org/pages/about.html*. Therefore, in order to retrieve files, a user must send out a request to collect and assemble pieces of that file from other user's data store.

C. The Indicator Used by Law Enforcement is Unreliable

As discussed above, Freenet retrieves files by sending out requests from a user to its peers to collect pieces of that file. That user's peers then forward the request for file pieces to their own sets of peers. The number of times a request can be forwarded is called the Hops to Live, or 'HTL'. The default maximum HTL is 18. Freenet hides the identity of the original requestor of a file by randomizing when the HTL of a request is forwarded as 17 or 18. A randomized HTL value is made for each peer-to-peer connection, not for the request as a whole. A peer receiving the original request forwards the randomized HTL value to the next node, which in turn forwards the request again, decrementing the HTL as it travels down a path.

The source code for Freenet is publicly available. The source code developed for rerouting each request, and how the process, called probabilistic decrement, works reads:

```
        /**
      * Decrement the HTL (or not), in accordance with our
      * probabilistic HTL rules. Whether to decrement is determined
        once for
      * each connection, rather than for every request, because if we
        don't
      * we would get a predictable fraction of requests with each
        HTL - this
      * pattern could give away a lot of information close to the
        originator.
      * Although it's debatable whether it's worth worrying about
        given all
      * the other information they have if close by ...
      * @param htl The old HTL.
      * @return The new HTL.
        */
public short decrementHTL(short htl) {short max = node.maxHTL();

        if(htl > max)
                htl = max;if(htl <= 0)
                return 0;if(htl == max) {
if(decrementHTLAtMaximum || node.disableProbabilisticHTLs)
        htl--;
        return htl;
        }
        if(htl == 1) {
if(decrementHTLAtMinimum || node.disableProbabilisticHTLs)
        htl--;
        return htl;
        }
        htl--;
        return htl;
```

Noting the included comment, the HTL is determined for each connection to a peer; the HTL is not the same for every peer that receives a part of the original request. As such, a peer may receive a number of different values. A receiving peer, forwarding an original request, may send out the request to its own set of peers with an HTL of 16 (if the peer received an HTL 17 request and decremented it), 17 (if the peer received an HTL 17 or 18 request and chose to decrement or not), or 18 (if the peer is just forwarding the original request without any decrement). Therefore, if law enforcement were to "receive a number of file requests with HTL values of 16 or 17 mixed with HTL 18s for the same file, it means HTL 18s are the result of randomly not decrementing the HTL and the subject IP is not the requestor." Missouri ICAC Task Force, *Black Ice: The Law Enforcement Freenet Project*, (September 2013) *https://retro64xyz.gitlab.io/assets/pdf/blackice_project.pdf*. (Attached hereto as Exhibit B.)

Conversely, "a number of HTL 18s for a file without any HTL 16/17s makes it highly likely that [the] subject is the requestor." *Id.*

The affidavit of probable cause states that "By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. A mathematical formula is applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer." Affidavit of Probable Cause p. 6. The first issue with this is that the affidavit gives no information on whether there were other requests from Mr. McEachern's node or how precisely it was determined that Mr. McEachern was the originator of the requests and not merely an intermediary.

In order to determine the true requestor, a law enforcement computer would need toestablish the HTL value of requests received and be able to track backwards to the source. However,

> [s]ince the only IP addresses known to the LEFnode [Law Enforcement node] are the ones directly connected to it, there is currently no way to tell what IP requested a key if the HTL is less than 18… There is also the possibility that a request with a HTL of18 is not from the originator but randomly (50/50 chance) passed along without being decremented. A feature, called probabilistic HTL, will change the HTL when at 18, or not decrement it, as it reroutes the request.

Id. This means that the law enforcement node has no way to track the IP addresses of the nodes that have forwarded the request. The only information law enforcement has is that they received a request from this specific IP address, with no history of where the request may have come from before that.

The potential for the peer sending the NCSBI the request to be the original requestor is also lowered when typical Freenet traffic is factored in. Requests for child pornography related documents accounts for 35% of all Freenet traffic. Brian Levine, Marc Liberatore, Brian Lynn, Matthew Wright, *Statistical Detection of Downloaders in Freenet*, (2017) (Attached hereto as Exhibit C.) With such a high volume of requests for child porn related documents, and those requests being forwarded multiple times, the chance for an IP address to unknowingly forward a request for child porn is high.

Therefore, Mr. McEachern asserts that the indicator that triggered this investigationis an unreliable method of selecting targets. The NCSBI has placed an undue amount of reliance on the reroute requests. As such, using this value as a method to decide which IP addresses to target is too broad.

The files allegedly requested by Mr. McEachern's IP address were videos with relatively large sizes. If those requests were only being forwarded by Mr. McEachern's node from another node with a limited number of peers, then there is a large chance for a false positive. The formula makes the assumption that the larger the requested piece of the file, the better chance of the original requestor. Therefore, not only is the trigger for the analysis unreliable, the formula itself is subject to false results.

III. CONCLUSION

For all the reasons set forth above, the evidence obtained on October 21, 2021 is not admissible under the Fourth Amendment to the Constitution. Mr. McEachern, by his counsel undersigned, respectfully requests that the Court grant this Motion and preclude the government from introducing the contested evidence.

Respectfully submitted, this the 22nd day of March, 2022.

/s/Helen L. Parsonage
Helen L. Parsonage (35492)
Elliot Morgan Parsonage, PLLC
426 Old Salem Road
Winston-Salem, NC 27101
(336) 724-2828
hparsonage@emplawfirm.com

CERTIFICATE OF SERVICE

I, Helen Parsonage, hereby certify that I have caused a copy of Defendant's Motion to Suppress Evidence Obtained in Violation of the Fourth Amendment, and Memorandum of Law in Support Thereof, to be filed and served electronically through the ECF system, upon the United States Attorney.

This the 21st day of March, 2022.

/s/Helen L. Parsonage
Helen L. Parsonage (35492)
Elliot Morgan Parsonage, PLLC
426 Old Salem Road
Winston-Salem, NC 27101
(336) 724-2828
hparsonage@emplawfirm.com